REMARKS

I. INTRODUCTION

Claims 1, 4 and 10 have been amended. No new matter has been added. Claims 1-21 remain pending in the present application. In view of the above amendments and the following remarks, it is respectfully submitted that all of the presently pending claims are allowable.

II. THE 35 U.S.C. § 112 REJECTION SHOULD BE WITHDRAWN

The examiner has objected to the original claim 4 under 35 U.S.C. § 112 as being indefinite. This rejection owed to the original claim's use of the term "likely," which could render the invention indefinite in the eyes of one of ordinary skill in the art. Claim 4 has been amended to comply with the formulation suggested in the rejection. Thus, it is respectfully submitted that the 35 U.S.C. § 112 rejection of claim 4 should be withdrawn.

III. THE 35 U.S.C. § 102(e) REJECTIONS SHOULD BE WITHDRAWN

Claims 1-5, 10 and 14-16 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,760,444 to Leung ("Leung"). (See 9/28/05 Office Action, pp. 3-7). Leung describes a process where a roaming device (termed a "mobile node") attempts to make contact with a first access point (termed a "Home Agent"). (See Leung, col. 7:11-22). The Home Agent communicates with an authentication server to obtain a security association for the mobile node, which is transmitted back to the Home Agent. (See Leung, col. 7:23-44). As the mobile node roams, attempting to access network resources via additional access points (termed "foreign agents"), those foreign agents communicate with the Home Agent, rather than with the authentication server, in order to authenticate the mobile node. (See Leung, col. 7:51-56). The authentication data is stored at the Home Agent in order to reduce the effort associated with retrieving the security association from the authentication server each time the mobile node sends a registration request. (See Leung, col. 7:56-61).

In contrast, claim 1 recites "generating, by an authentication server of the network, authentication data associated with the roaming device," "sending, by the authentication server, the authentication data to access points of the network, the access points being connected to the authentication server" and "when the roaming device roams to a particular access point of the access points, using the authentication data to locally authenticate the roaming device at the particular access point." Thus, the recitation of claim 1 is a method of authentication where the authentication server sends authentication data to multiple access points, in order that authentication can be accomplished locally at any individual access point, without further communication with the authentication server or any other access point that might serve as a Home Agent.

Leung neither discloses or suggests such a method, wherein all or multiple access points receive the authentication data from the authentication server for a particular roaming device. In various parts of the rejection, the Examiner points to the description with reference to Fig. 5 of Leung to support the contention that Leung teaches the same authentication data being stored at multiple Home Agents. However, Fig. 5 and its corresponding description clearly show that the system being described does not include an authentication server to generate authentication data. (See Leung, col. 4:32-56). The system being described with reference to Fig. 5 is a system that has individually stored authentication tables at each Home Agent, but these tables are not generated by an authentication server. In fact, Leung states that "the security-association tables are typically manually configured for each Home Agent." (See Leung, col. 4:32-33)

Where Leung discloses a centralized authentication server (Figs. 6-8 and corresponding description), Leung only teaches that the authentication data is sent to the particular Home Agent for the mobile node. Again, the Examiner indicates in the rejection that this portion of Leung teaches sending the authentication data to multiple Home Agents. However, applicants respectfully disagree. There is absolutely no teaching that an authentication server sends authentication data to multiple Home Agents for a mobile node. In fact, this is the direct opposite of the Leung teaching that a mobile node is associated with a single Home Agent and any foreign agents that need to authenticate the mobile node must contact the Home Agent.

Accordingly, Leung neither teaches nor suggests "sending, by the authentication server, the authentication data to access points of the network, the access points being connected to the authentication server" and "when the roaming device roams to a particular access point of the access points, using the authentication data to locally authenticate the roaming device at the particular access point," as recited in claim 1. Therefore, applicants respectfully request that the 35 U.S.C. § 102(e) rejection over Leung be withdrawn. Because claims 2-5 depend from, and therefore include all the limitations of claim 1, it is respectfully submitted that these claims are also allowable.

Similar to claim 1, claim 10 recites "distributing, by the authentication server, the authentication data to the first access point and a second access point of the network" and "locally authenticating the roaming device upon a contact with the second access point using the distributed authentication data." Thus, for at least the reasons discussed with reference to claim 1, claim 10 is also allowable. Because claims 14 and 15 depend from, and therefore include all the limitations of claim 10, it is respectfully submitted that these claims are also allowable.

Also similar to claim 1, claim 16 recites a system including an authentication server and two access points "wherein the authentication server sends the authentication data to the first and second access points upon an initial authentication procedure of the roaming device with the first access point and wherein the second access point locally authenticates the roaming device upon a contact of the roaming device with the second access point." Thus, for at least the reasons discussed with reference to claim 1, claim 16 is also allowable.

Claims 1-3, 6, 10-12, 14 and 16-18 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,851,050 to Singhal et al. ("Singhal") (See 9/28/05 Office Action, pp. 7-11). Singhal describes an authentication method whereby an access point that has been contacted by a roaming device (termed a "client") communicates with an authentication server in order to authorize the client. (See Singhal, col. 18:39-60). Once this initial authentication has taken place, authentication data is stored with a routing coordinator which operates in parallel with the authentication server and, like the authentication server, is dominant over the various access points.

(See Singhal, col. 18:61-64 and Fig. 14). When the client attempts to begin communications with a new access point, said new access point must communicate with the routing coordinator or the authentication server in order to properly identify and authenticate the client. (See Singhal, cols. 18:65-19:1).

As described above, claim 1 recites an authentication method whereby authentication data is transmitted from the authentication server directly to access points, such that further authentication processes can be performed locally rather than requiring additional upstream communication with the authentication server or any other upstream device such as the routing coordinator described in Singhal. Thus, Singhal neither teaches nor suggests a method where subsequent authentication is performed locally at the access points without referring to upstream computing resources.

Accordingly, it is respectfully submitted that claim 1 is allowable over Singhal. Because claims 2, 3 and 6 depend from, and therefore include all the limitations of claim 1, it is respectfully submitted that these claims are also allowable.

As described above, claim 10 includes limitations similar to claim 1 such that authentication data is transmitted directly from the authentication server to multiple access points, so that authentication can be performed locally at the access points. As stated above in the discussion of claim 1, Singhal neither teaches nor suggests such a method. Thus, it is respectfully submitted that claim 10 is allowable over the '050 patent. Because claims 11, 12 and 14 depend from, and therefore include the limitations of claim 1, it is respectfully submitted that these claims are also allowable.

Similarly, claim 16 recites a system for performing the method recited in claim 10. The system of claim 16 shares the capability of performing authentication locally at the access points once an initial communication with the authentication server has taken place. Thus, it is respectfully submitted that claim 16 is allowable over the '050 patent. Because claims 17 and 18 depend from,

and therefore include the limitations of claim 16, it is respectfully submitted that these claims are also allowable.

IV. THE 35 U.S.C. § 103(a) REJECTIONS SHOULD BE WITHDRAWN

Claims 7, 8 and 13 stand rejected under 35 U.S.C. § 103(a) as unpatentable over the Singhal in view of U.S. Patent No. 6,452,910 to Vij et al. ("Vij"). (See 9/28/05 Office Action, pp. 11-14). Vij does not cure the above described deficiencies of Singhal. Accordingly, because claims 7 and 8 indirectly depend from claim 1, for the reasons stated above with respect to claim 1, it is respectfully submitted that claims 7 and 8 are allowable. Similarly, claim 13 depends from claim 10 and therefore, for the reasons stated above with respect to claim 10, it is respectfully submitted that claim 13 is allowable.

Claim 9 stands rejected under 35 U.S.C. § 103(a) as unpatentable over Singhal. (See 9/28/05 Office Action, pp. 14-15). Because claim 9 depends on claim 1, for the reasons stated above with respect to claim 1, it is respectfully submitted that claim 9 is allowable.

Claims 15, 19 and 20 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Singhal in view of U.S. Patent No. 6,633,761 to Singhal et al. ("Singhal II"). (See 9/28/05 Office Action, pp. 15-17). Singhal II does not cure the above described deficiencies of Singhal. Accordingly, because claim 15 depends from claim 10, for the reasons stated above with respect to claim 10, it is respectfully submitted that claim 15 is allowable.

Claim 19 recites an authentication method including "with an authentication server, receiving an authentication request from a roaming device, the request being encrypted with a first shared code," "with the authentication server, generating a session key associated with the roaming device," "sending the session key to an access point of the network, the session key being encrypted with a second shared code" and "utilizing the session key to authenticate the roaming device at the access point, and to encrypt data exchanged between the roaming device and the access point."

Thus, claim 19 recites an an authentication request, encrypted with a first shared code, and a session key encrypted with a second shared code.

Singhal II teaches the use of a security protocol, such as the RADIUS protocol, to protect authentication data, such as those used in an authentication process such as that taught by Singhal. However, neither Singhal or Singhal II teach or suggest a method where the authentication data is transmitted to the authentication server using a first shared code, and from the authentication server using a second shared code. Thus, it is respectfully submitted that claim 19 is allowable over Singhal and Singhal II. Because claim 20 depends from, and therefore includes all the limitations of claim 19, it is respectfully submitted that this claim is also allowable.

Claim 21 stands rejected under 35 U.S.C. § 103(a) as unpatentable over Singhal in view of Singhal II and in further view of U.S. Patent No. 6,178,506 to Quick, Jr. ("Quick, Jr."). (See 9/28/05 Office Action, pp. 17-18). Quick Jr. does not cure the above described deficiencies of Singhal and Singhal II. Thus, because claim 21 depends from, and therefore includes the limitations of claim 19, it is respectfully submitted that this claim is also allowable.

CONCLUSION

In light of the foregoing, Applicants respectfully submit that all of the now pending claims are in condition for allowance. All issues raised by the Examiner having been addressed, an early and favorable action on the merits is earnestly solicited.

Respectfully submitted,

Dated: December 22, 2005

By: _____
Oleg F. Kaplun (Reg. No. 45,559)

Fay Kaplun & Marcin, LLP
150 Broadway, Suite 702
New York, New York 10038
Tel: (212) 619-6000
Fax: (212) 619-0276